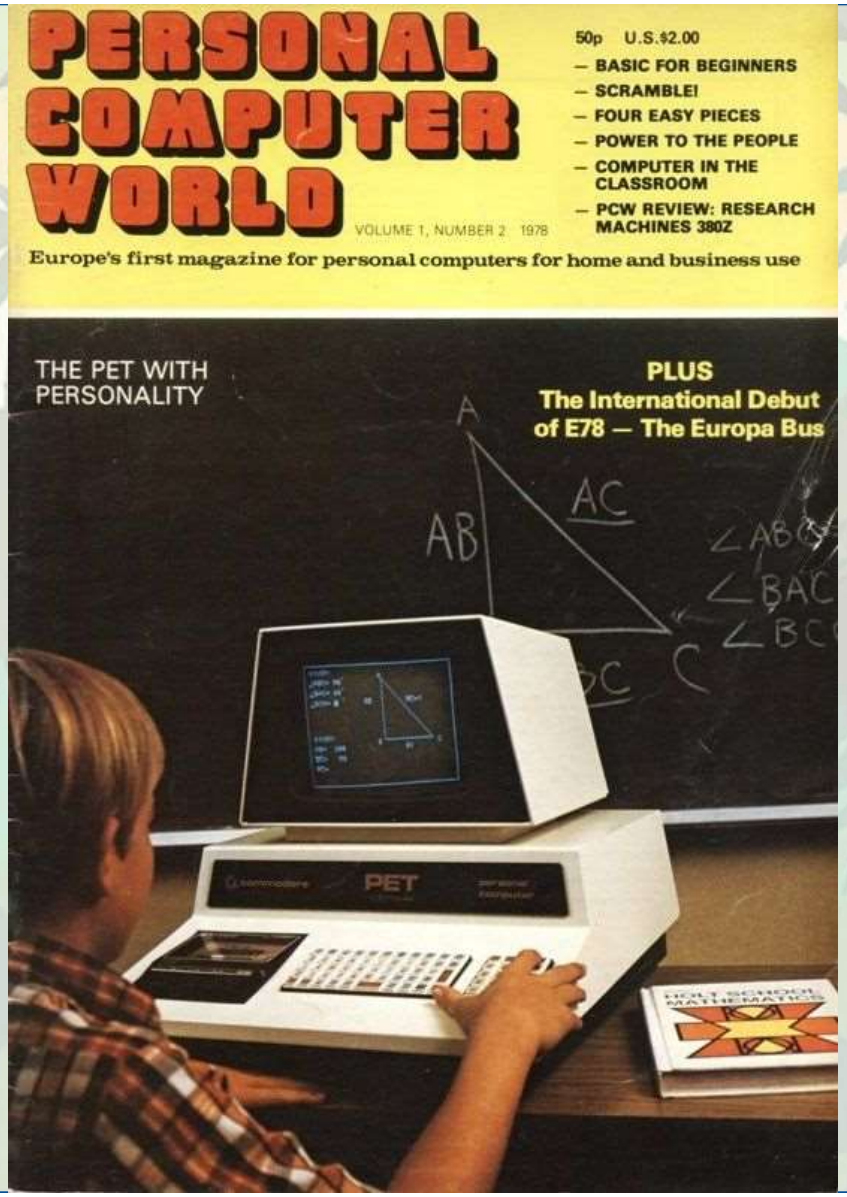
FUN WITH APPLICATION SECURITY

Bruce Abernethy

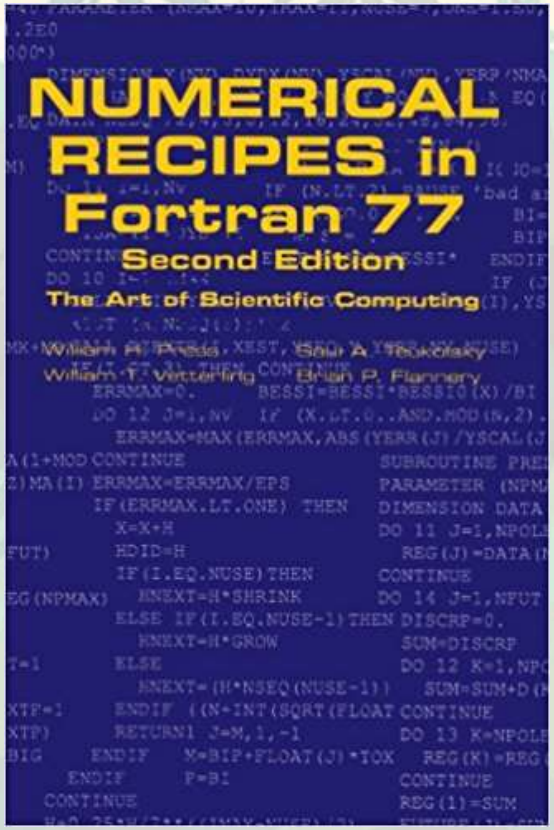
for BeerCityCode 2017

MY FIRST TIME CODING
1978



Programming on the P.E.T

FIRST SECURITY EXPERIENCE - 1988

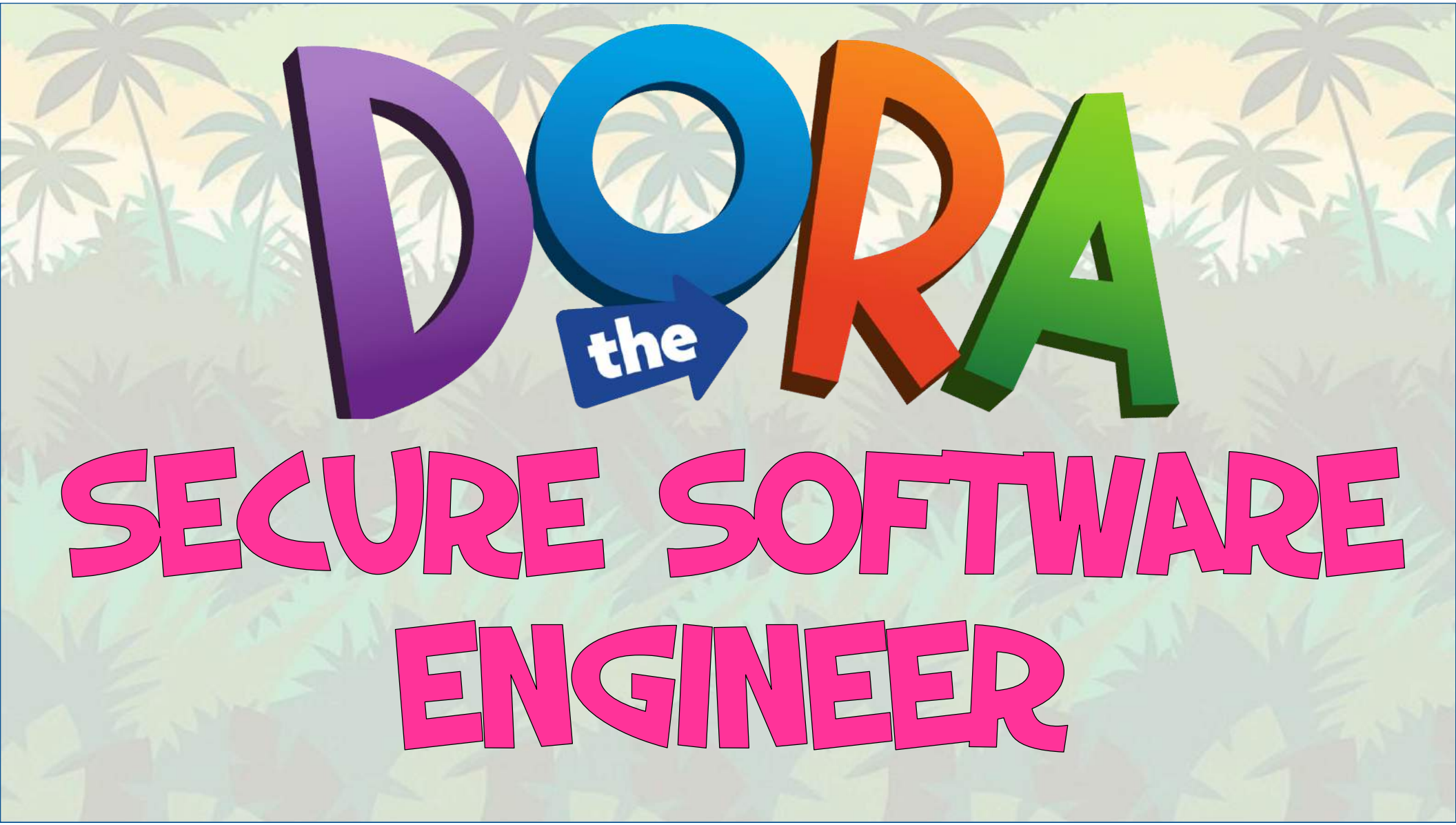


APPLICATION SECURITY IN 2018

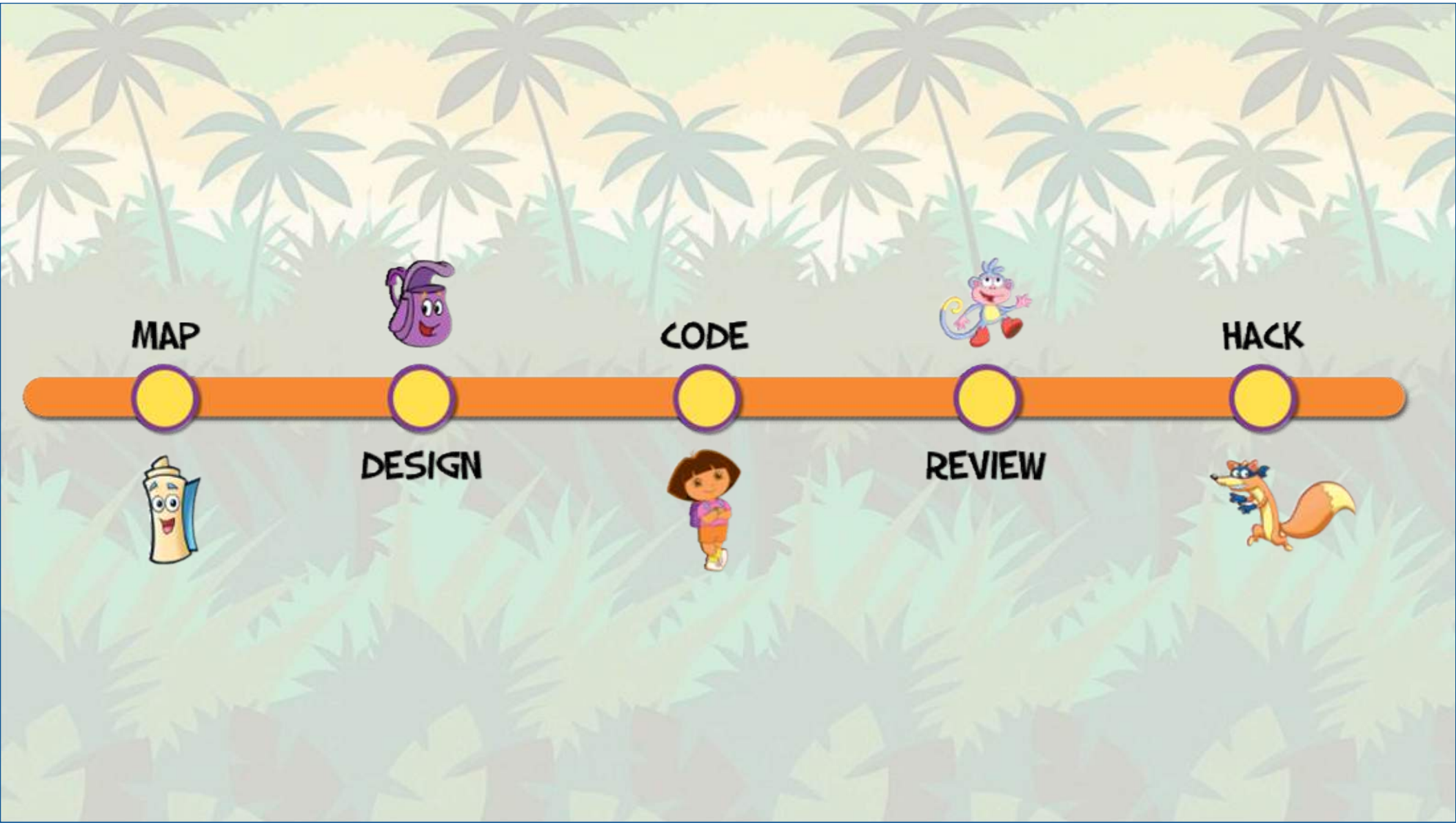

MAKE SOFTWARE
DEVELOPMENT FUN AGAIN

CONTENT WARNING

WARNING: THE FOLLOWING CONTENT AND OPINIONS EXPRESSED ARE THOSE OF THE AUTHOR [BRUCE ABERNETHY] AND TO NOT REFLECT THOSE OF HIS EMPLOYER [MEIJER] OR [DISNEY/NICKJR]

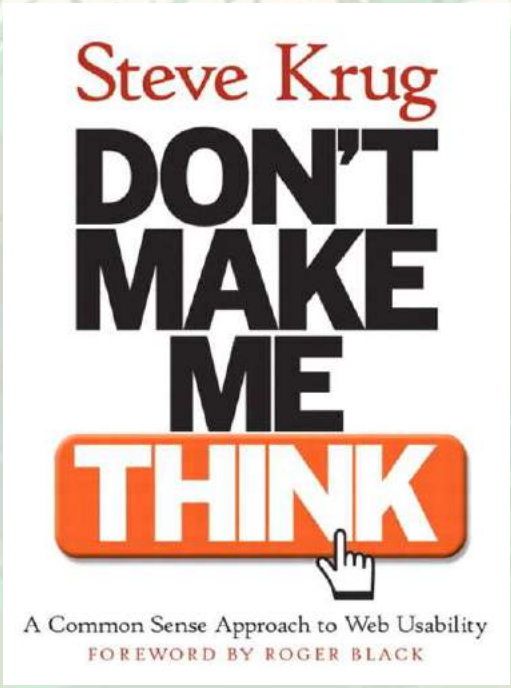

DORA
the
SECURE SOFTWARE
ENGINEER

TIC TAC TICO

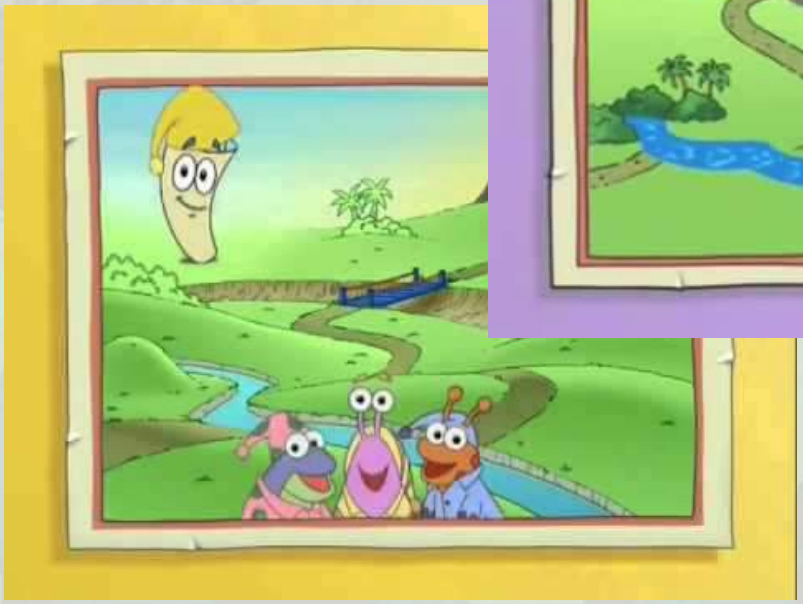

MAP
DESIGN
CODE
REVIEW
HACK

WHAT MAKES IT "FUN"

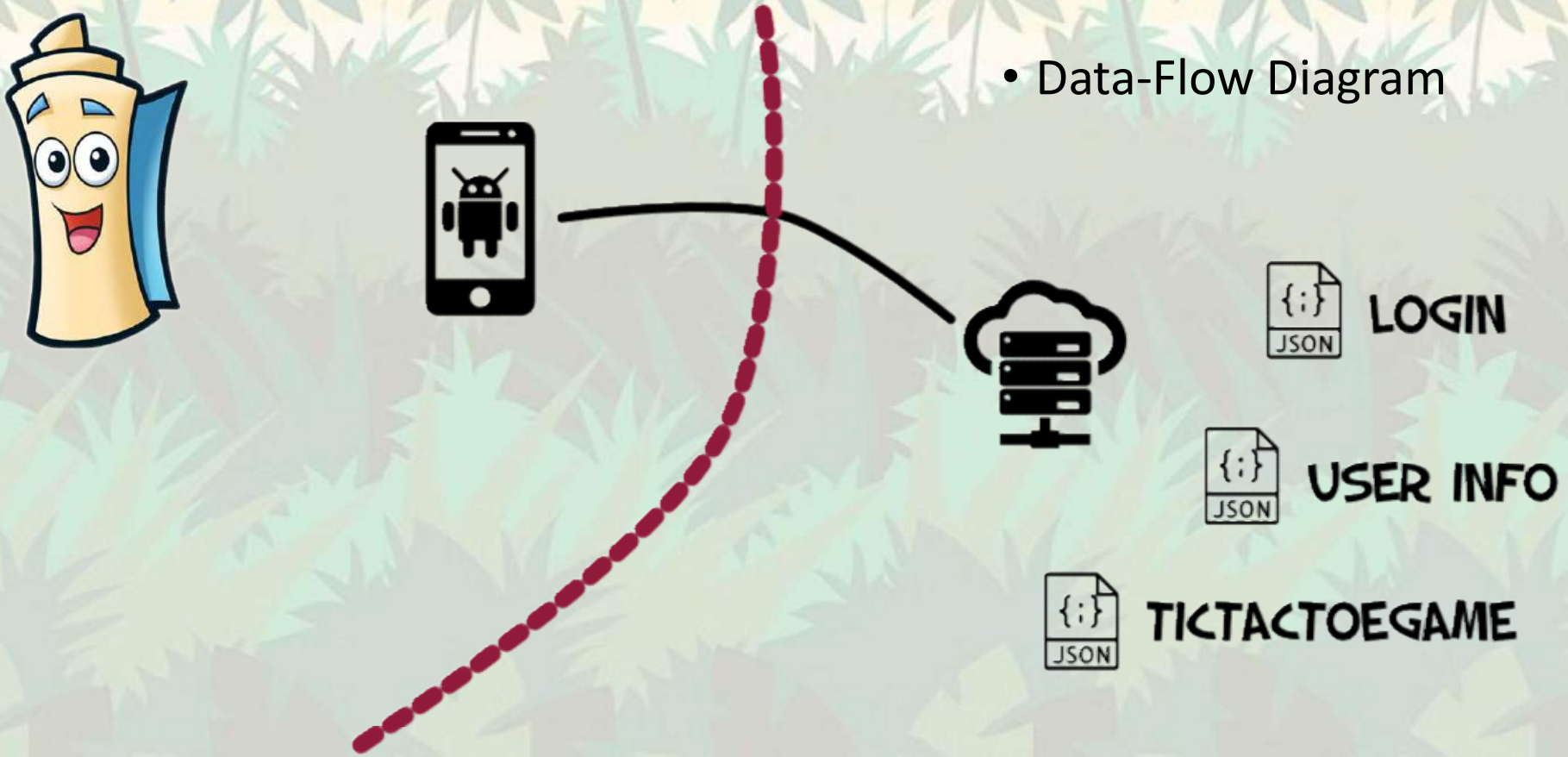
- Automation
- "AI"
- Rules
- Tools




MAP
DESIGN
CODE
REVIEW
HACK

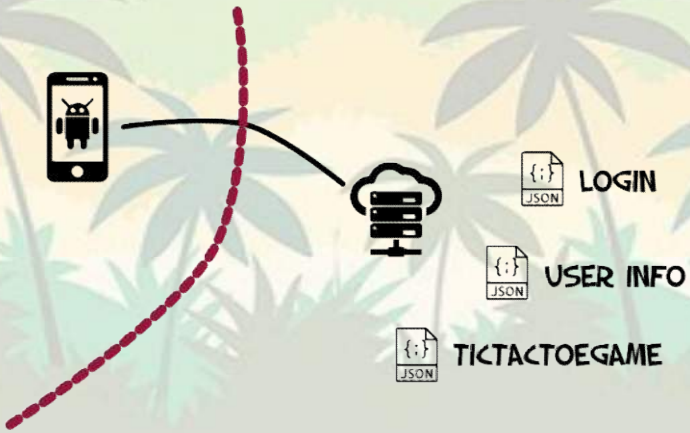


HIGH LEVEL DIAGRAM



- Data-Flow Diagram

STRIDE AND DREAD



STRIDE

- Spoofing Identity,
- Tampering with Data,
- Repudiation,
- Information Disclosure,
- Denial of Service

DREAD

- Damage Potential,
- Reproducibility,
- Exploitability,
- Affected Users,
- Discoverability

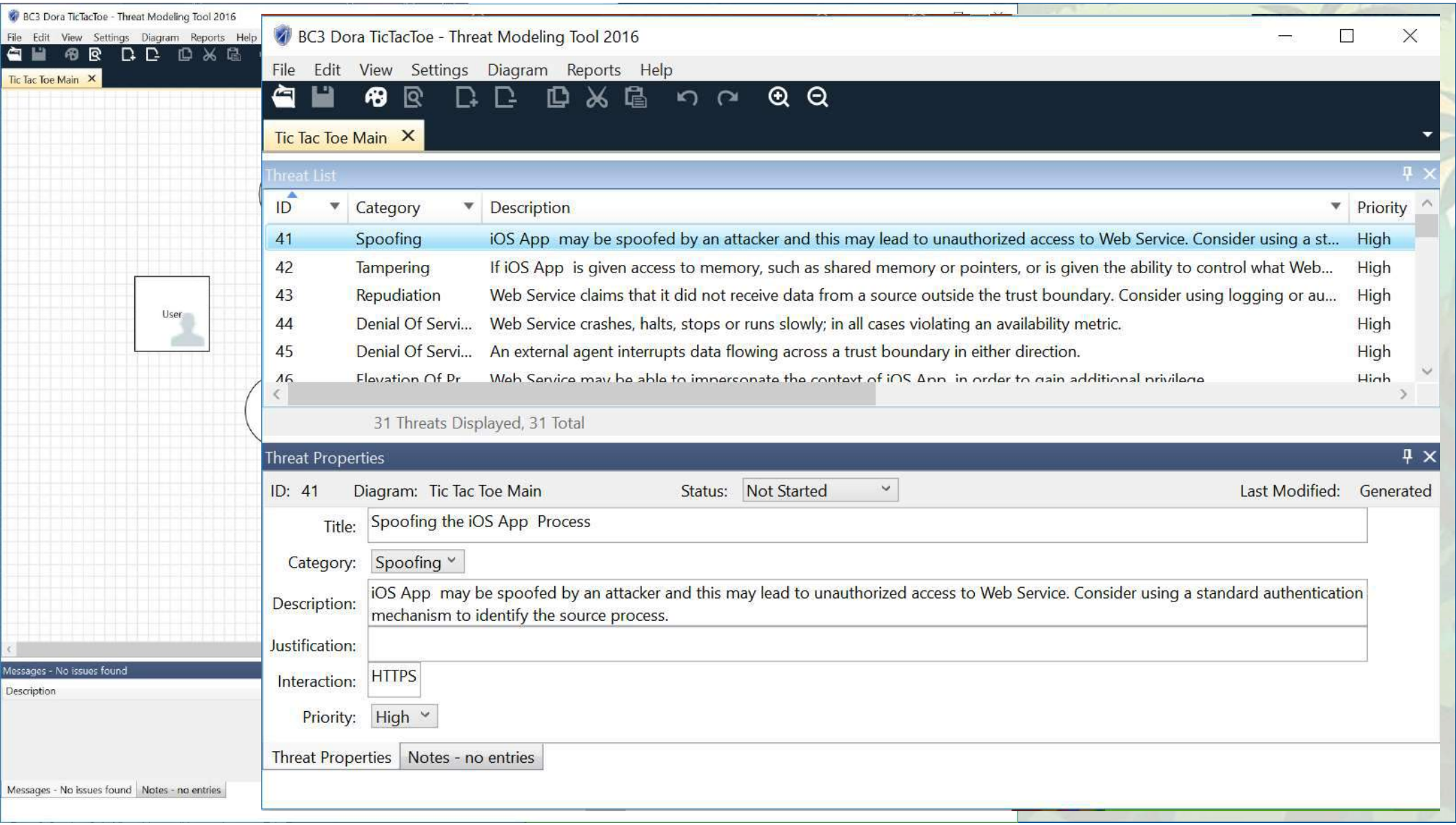
THREAT MODEL

- Have a high-level design. Napkin to formal tool.
- Data is exposed in primarily three places
  - At rest – wherever you store it
  - In memory – when it is being used
  - In transit – when it is moving
- Trust boundaries

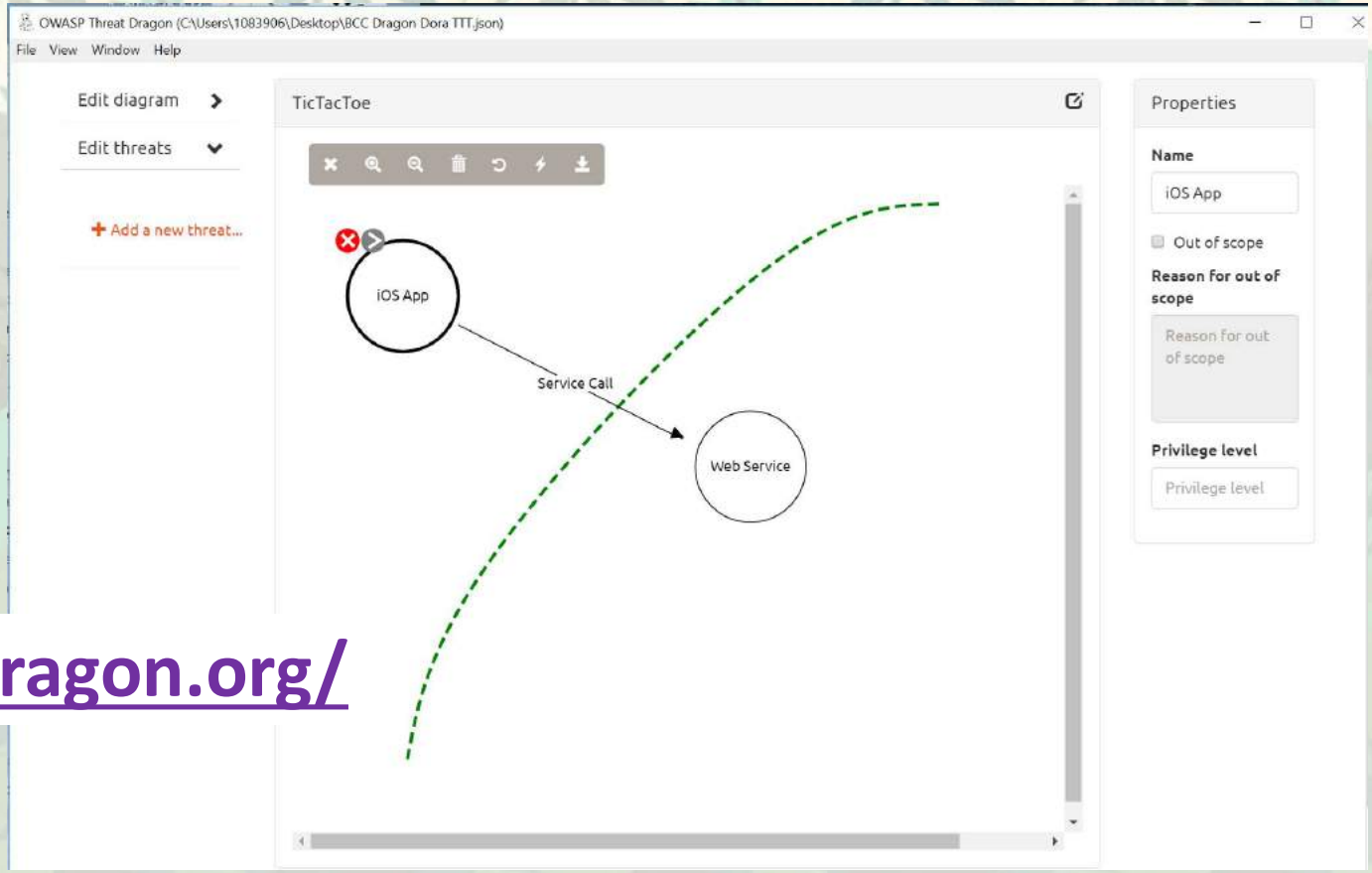
WHAT'S NOT FUN

- Doing the diagram by hand (Visio, Paint, GIMP).
- Doing the analysis by hand.
- Easily missing something.
- Not having time.

THREAT MODELLING TOOL


BC3 Dora TicTacToe - Threat Modeling Tool 2016
File Edit View Settings Diagram Reports Help
Tic Tac Toe Main
User
Messages - No issues found
Description
Messages - No issues found
Notes - no entries
BC3 Dora TicTacToe - Threat Modeling Tool 2016
File Edit View Settings Diagram Reports Help
Tic Tac Toe Main
Threat List
ID
Category
Description
Priority
41 Spoofing iOS App may be spoofed by an attacker and this may lead to unauthorized access to Web Service. Consider using a st... High
42 Tampering If iOS App is given access to memory, such as shared memory or pointers, or is given the ability to control what Web... High
43 Repudiation Web Service claims that it did not receive data from a source outside the trust boundary. Consider using logging or au... High
44 Denial Of Servi... Web Service crashes, halts, stops or runs slowly; in all cases violating an availability metric. High
45 Denial Of Servi... An external agent interrupts data flowing across a trust boundary in either direction. High
31 Threats Displayed, 31 Total
Threat Properties
ID: 41
Diagram: Tic Tac Toe Main
Status: Not Started
Last Modified: Generated
Title: Spoofing the iOS App Process
Category: Spoofing
Description: iOS App may be spoofed by an attacker and this may lead to unauthorized access to Web Service. Consider using a standard authentication mechanism to identify the source process.
Justification:
Interaction: HTTPS
Priority: High
Threat Properties
Notes - no entries

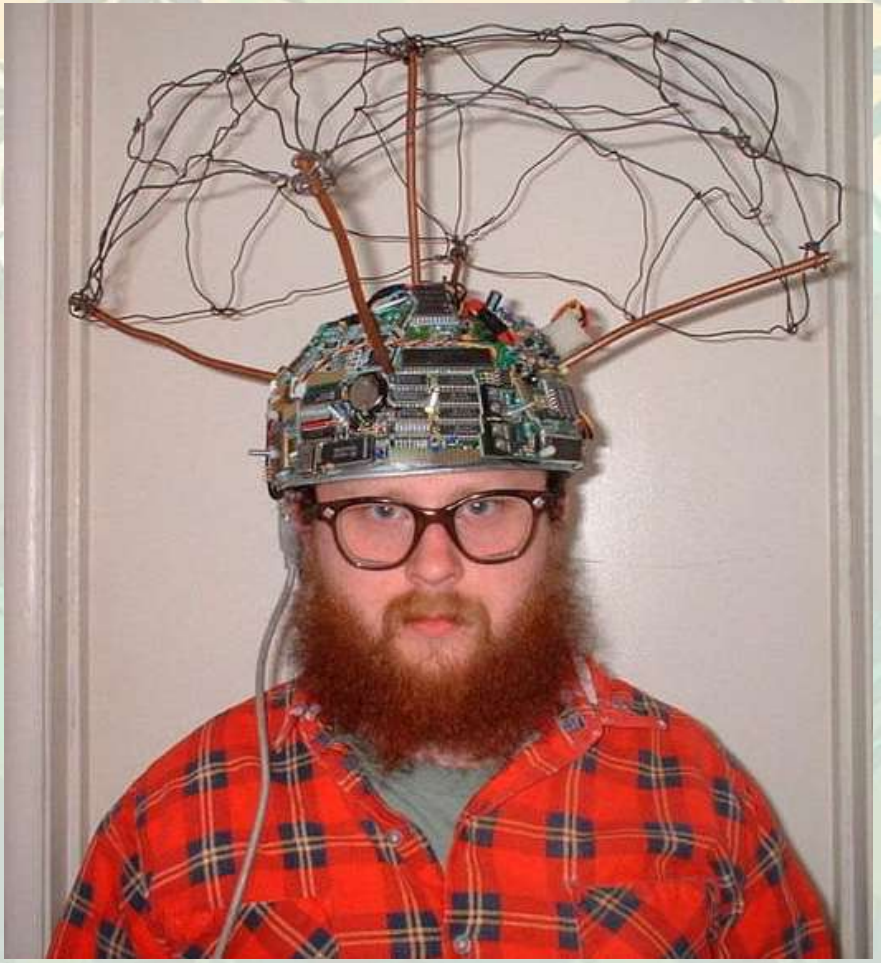
OWASP THREAT DRAGON (BETA - X-PLAT)

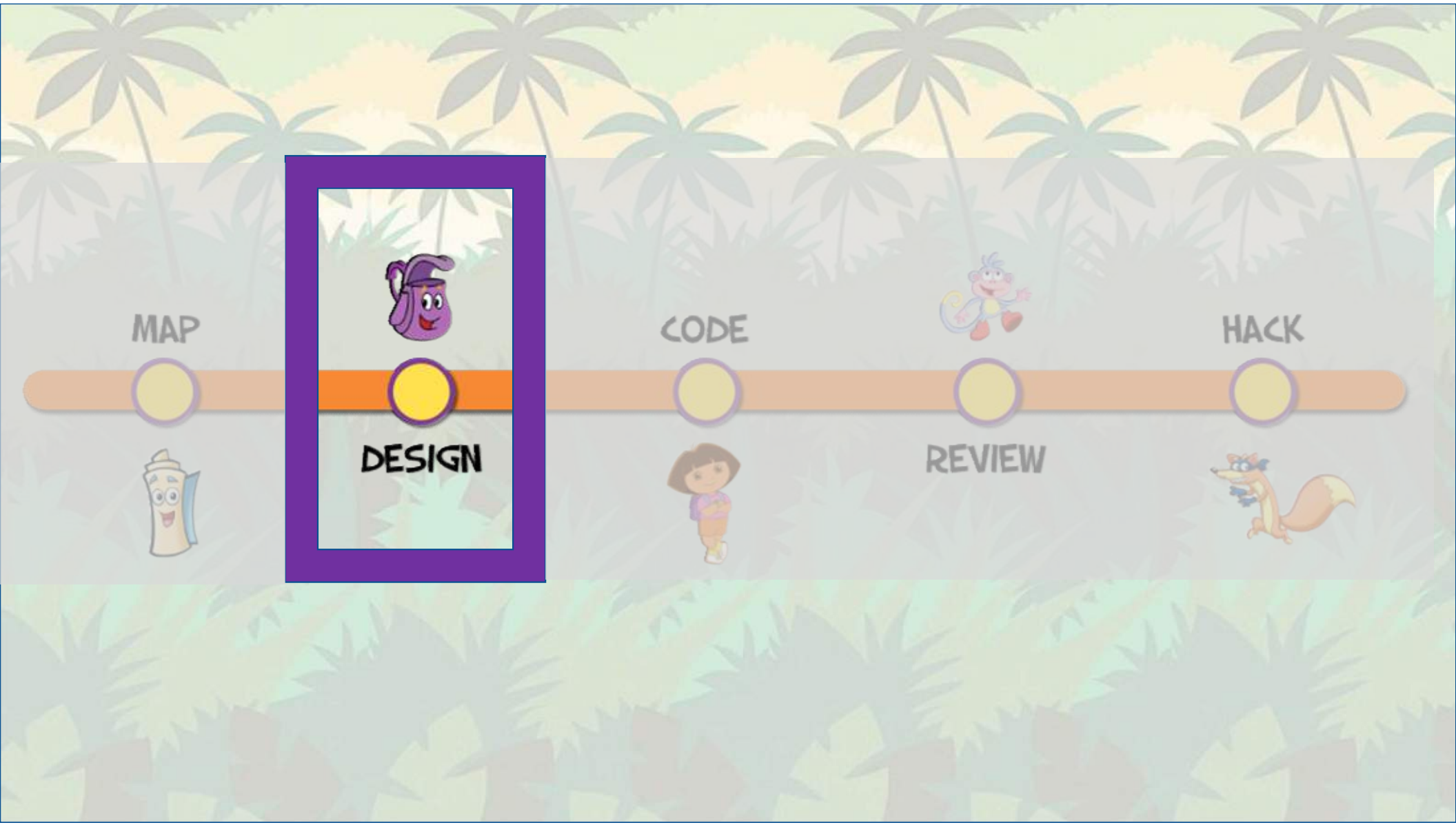


https://threatdragon.org/

SECURITY HAT ON

"Just because you are paranoid doesn't mean that they aren't watching you."



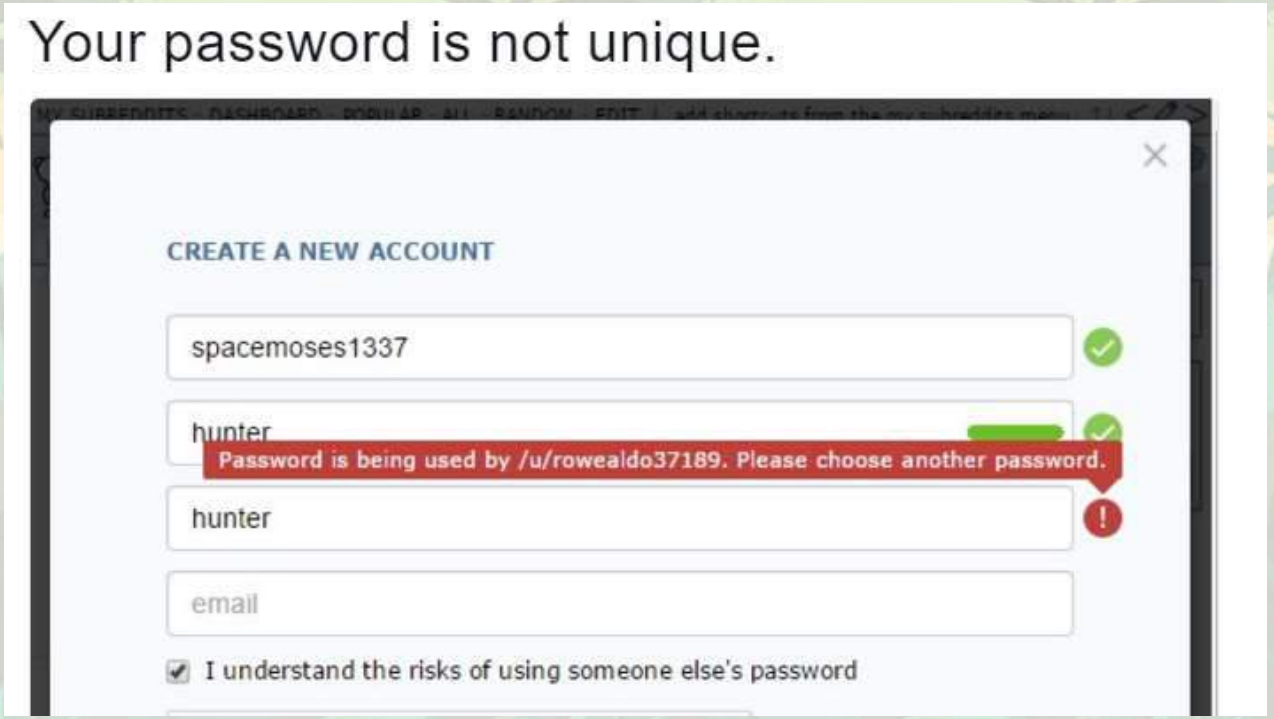

MAP
DESIGN
CODE
REVIEW
HACK

DESIGNING A SECURE APP

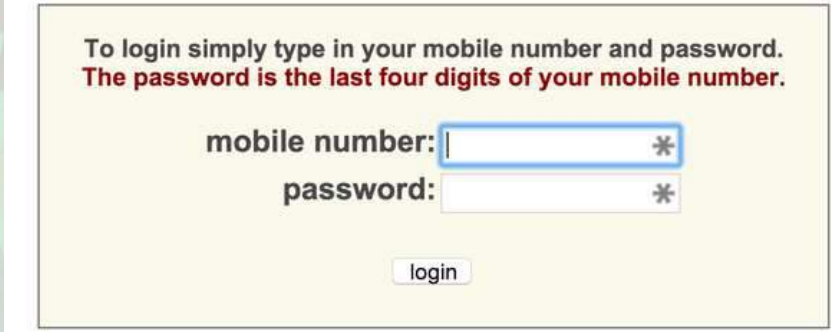
- Secure Coding “Level 0” is good coding.
- Much of malicious coding can appear at the outset like simply really bad coding practices
- Also User Interface
  - Well-meaning UI choices can be bad for security

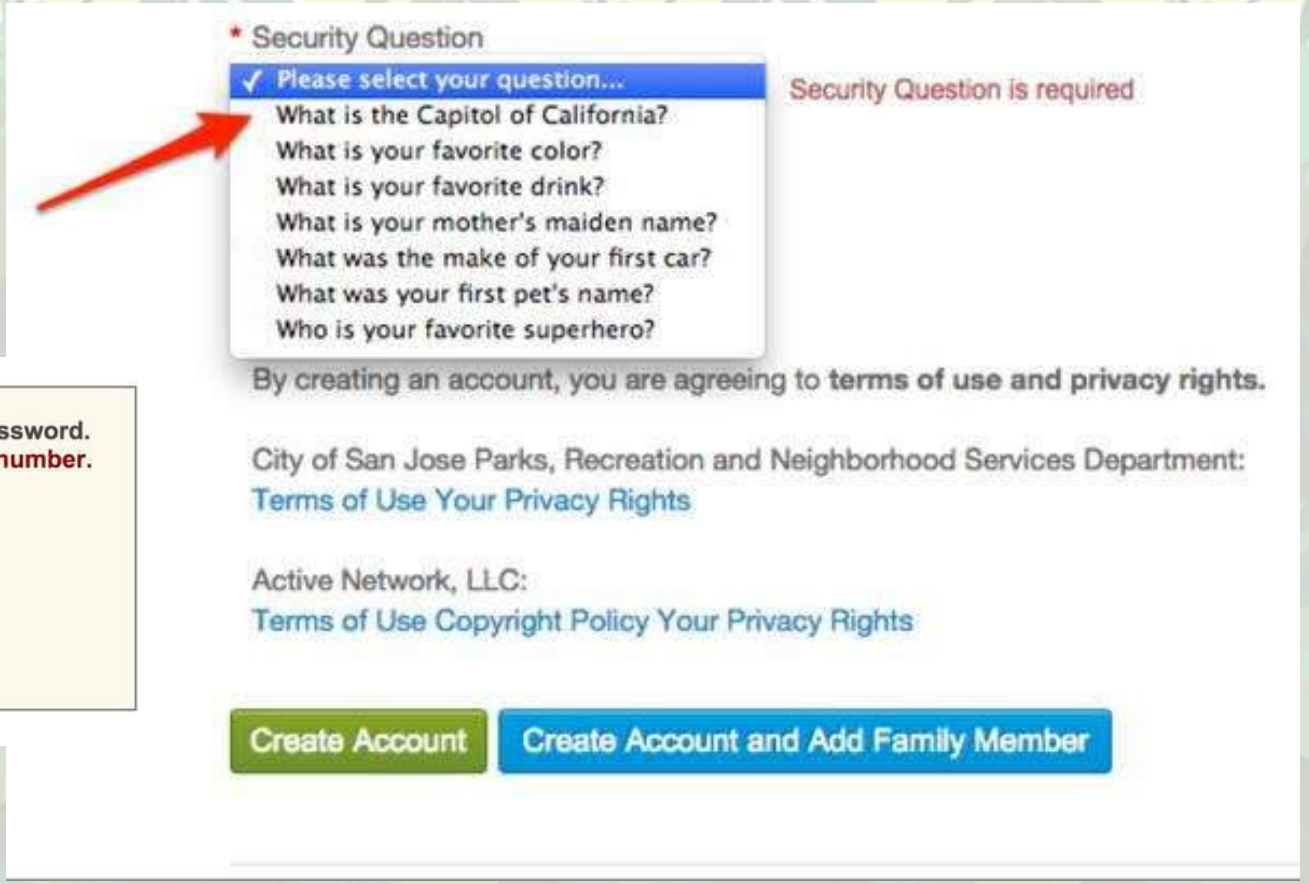
INFORMATION DISCLOSURE

- Most is common sense
- Don’t return error details
- Don’t return info that could be used “for evil”



OTHER GREAT (NOT) EXAMPLES





DESIGN GUIDANCE

OWASP

Open Web Application Security Project

- OWASP Top 10
- SANS Top 25

WHAT'S NOT FUN

- Figuring this stuff out on your own
- It is wise to learn from your mistakes. It is wiser to learn from other people's mistakes

OWASP TOP 10

- **Injection**
- **Cross-Site Scripting (XSS):**
- Vulnerability that is created from insecure coding techniques, resulting in improper input validation. Often used in conjunction with CSRF and/or SQL injection.
- **Insecure Direct Object References**
- A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

MAP

DESIGN

CODE

REVIEW

HACK

HELP WHILE CODING

- This is where the real fun happens
  - Adding features
  - Optimizing code

WHAT'S NOT FUN

- Reviewing 10,000 lines of code looking for patterns that might match common vulnerabilities (OWASP, SANS, etc.)
- Finding out after coding an entire feature that it has a fundamental security flaw and needs to be refactored or rewritten.
- Having the feature reach production and having to respond to a major incident.

TOOLS

- What tools should you have in your backpack, to help you along the way?
- "Anything that you might need, I've got inside for you.“
- Binoculars, sticky tape
- Bag of Holding

STATIC ANALYSIS TOOLS

- Client-Side (Microsoft)
  - Roslyn,
  - Resharper,
  - DevSkim,
  - PumaScan
- Client-Side (VS Code, DevSkim)
  - Cross-platform

DEBUGGING WITH PROXIES

- We are going to cover our favorite proxies in just a few minutes when we are hacking our own code.
- Just remember that you can/could/should be using a proxy, where appropriate, even early while you are developing code …

AUTOMATED TESTING - SECURITY TEST CASES

- Use Cases
- But also “Abuse Cases”
- Testing the happy path
- But also think about the unhappy path that “bad people” might take – more suggestions on how to do that coming soon too …

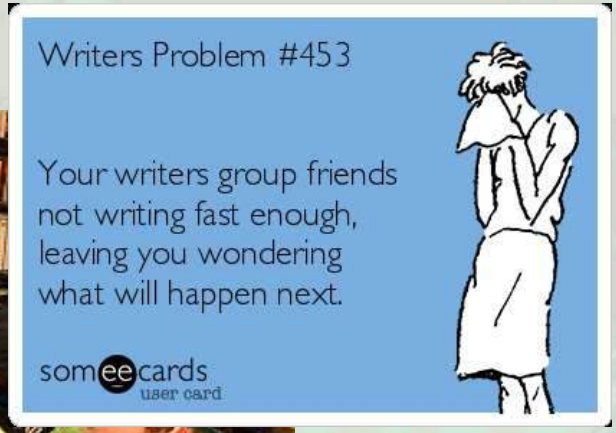

MAP
DESIGN
CODE
REVIEW
HACK


NEVER CODE ALONE

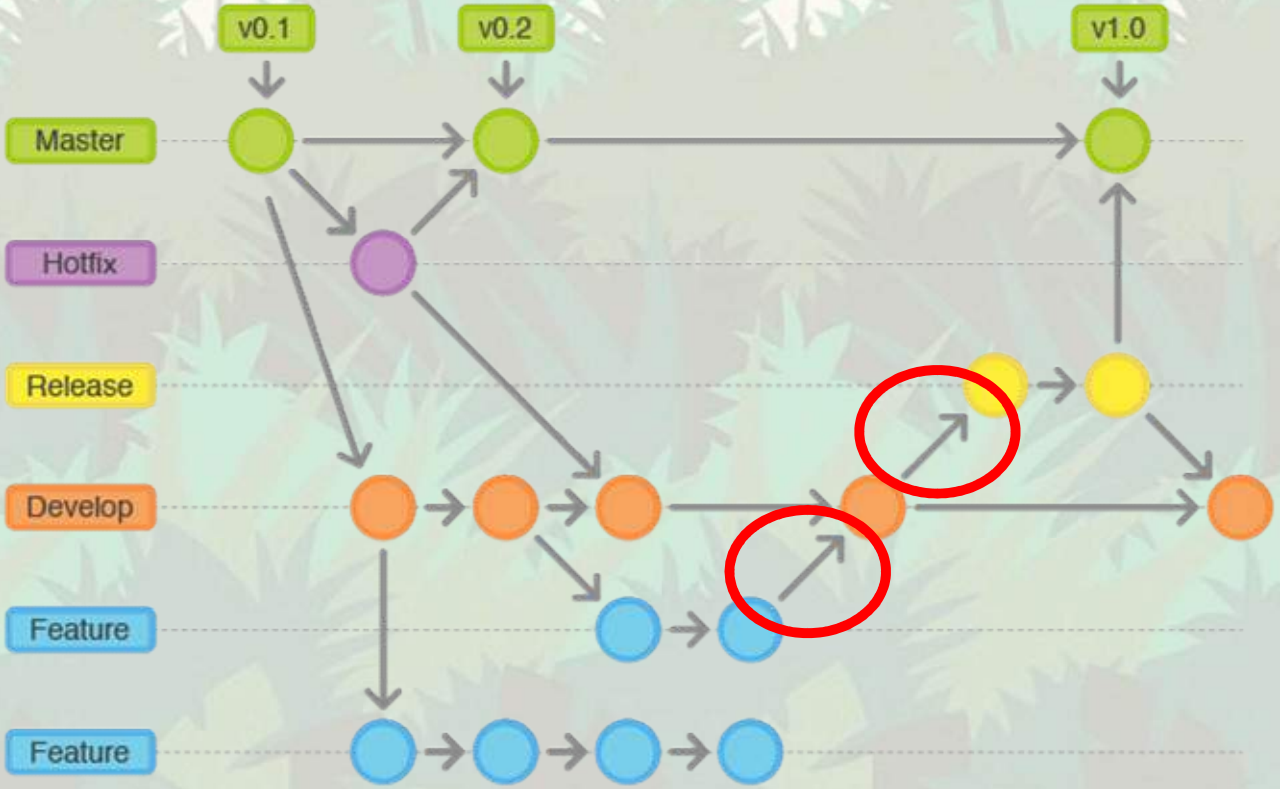

WHAT'S NOT FUN

CODING BUDDY

- Code & Coffee
- Personal Pull Requests



GITFLOW AND PULL REQUESTS ...



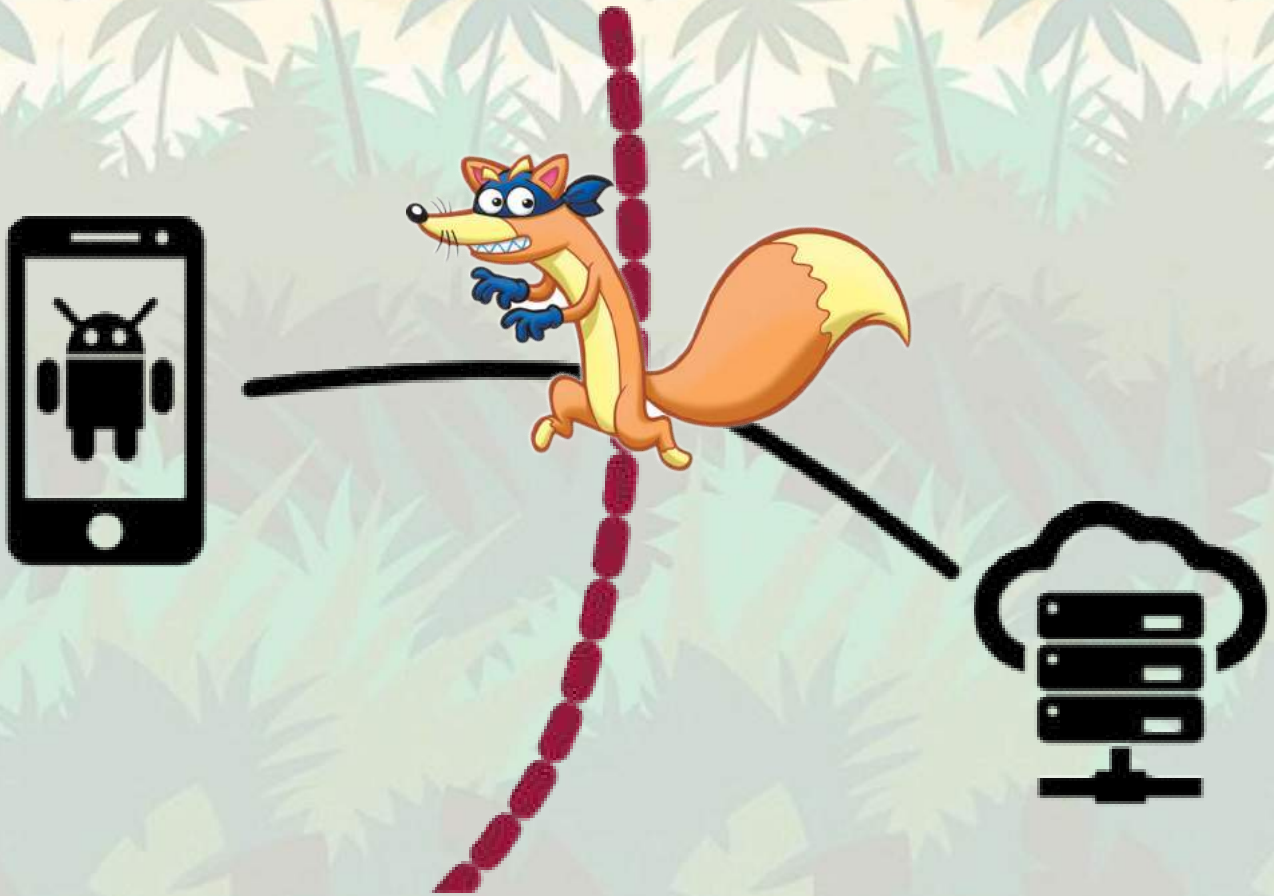

MAP
DESIGN
CODE
REVIEW
HACK

KNOW YOUR THREATS

- **Script kiddies** – hobby – opportunistic, not stealthy, known exploits
- **Organized Crime** – hold hostage, profit – possibly stealthy, often non-targeted / broad, zero-day – may target for corporate espionage
- **Disorganized Crime** – petty theft, personal gain – amateur, known
- **Activist** – do damage, get press – mixed, disgruntled
- **Nation-state** – destabilize, do damage – more skilled than you, targeted, precise, zero-day exploits

WHAT IS YOUR "GOLD"

MAN IN THE MIDDLE (MITM)



MAN IN THE MIDDLE (MITM)

- CERT
- AES
- SSL/TLS – Https everywhere (certificates in general)
- NIST
- YubiKey
- Oauth2 – everywhere
- 2-factor - multifactor
- nmap

TRAFFIC INSPECTION / INTERCEPTION

- Fiddler
- OWASP ZAP
- BURP Suite
- Swagger

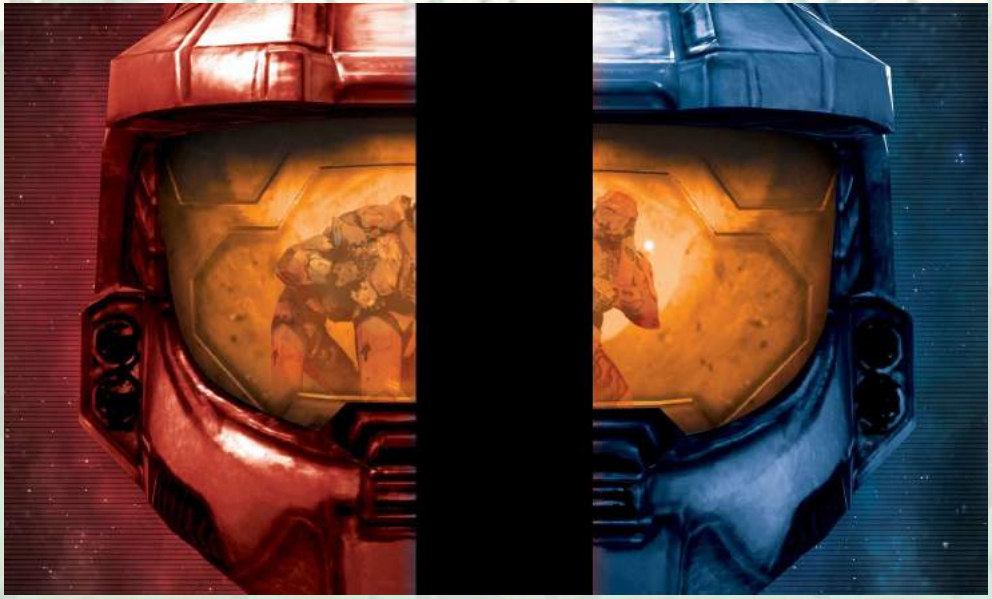
BOTS

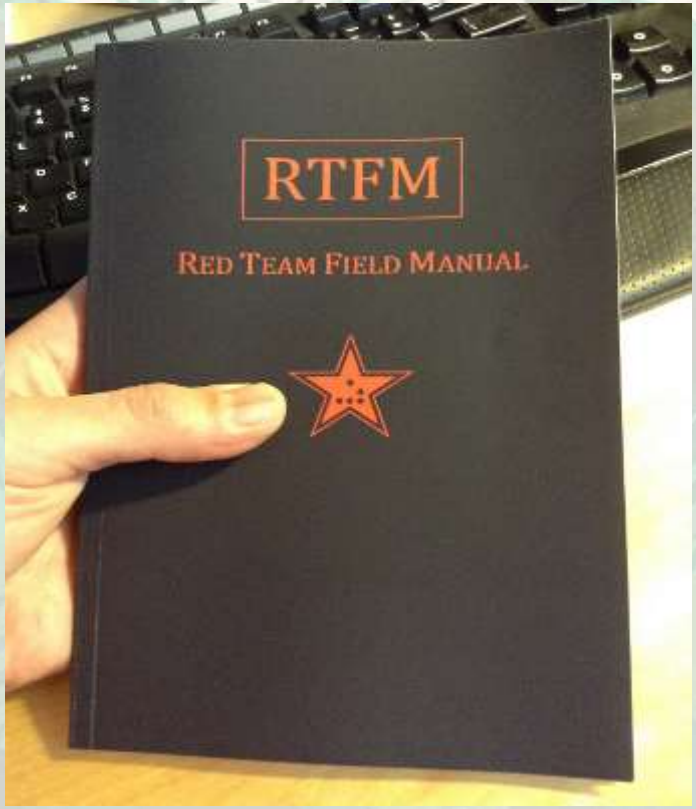
- Scanners
- Fuzzers
- Brute Force

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

DEMO

RED TEAM / BLUE TEAM

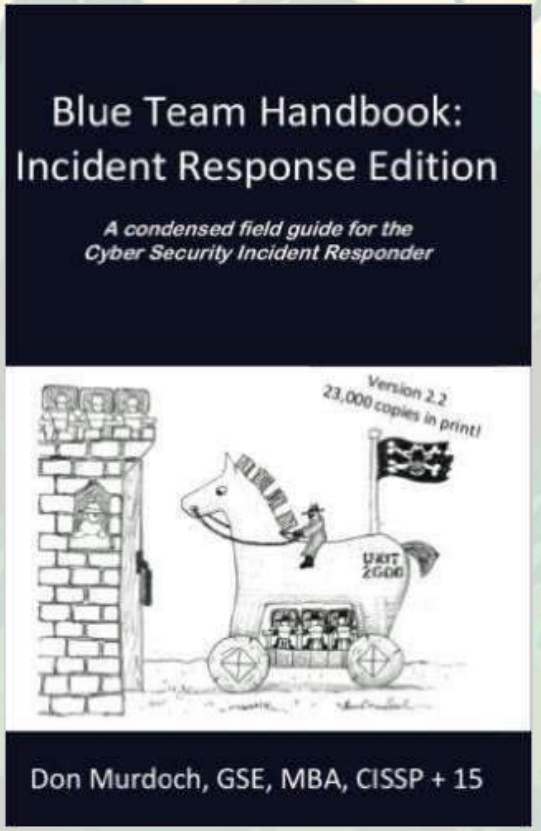


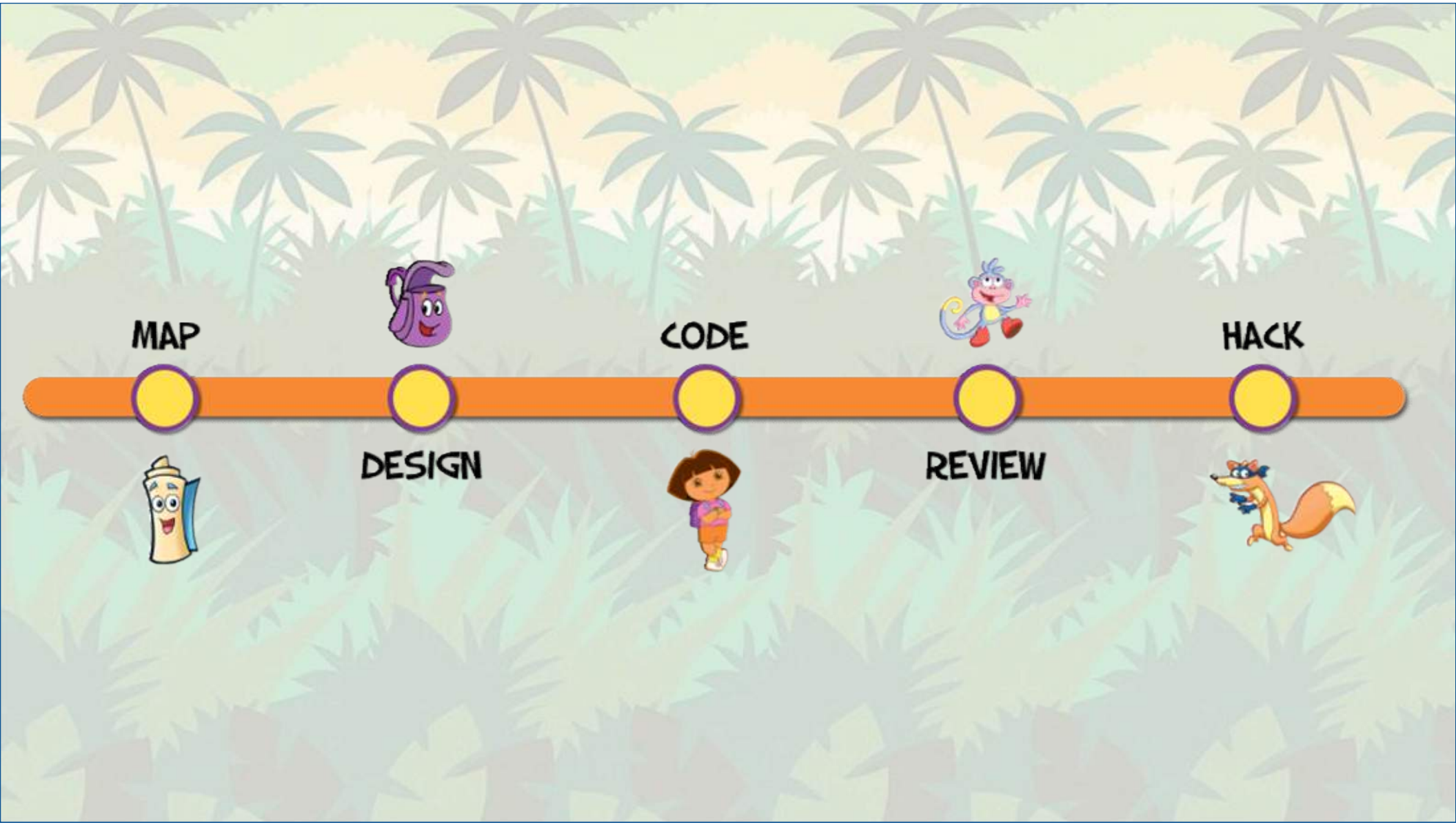


- Hack yourself and/or your coding buddy.

BLUE TEAM

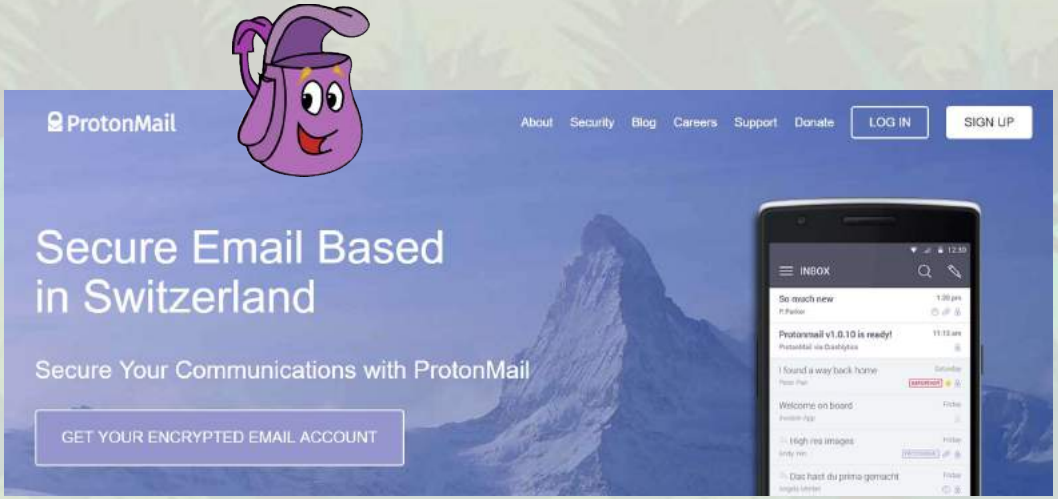
- Lesser known, but also cool.
- Ideas like Honeypots




MAP
DESIGN
CODE
REVIEW
HACK

SECURE E-MAIL

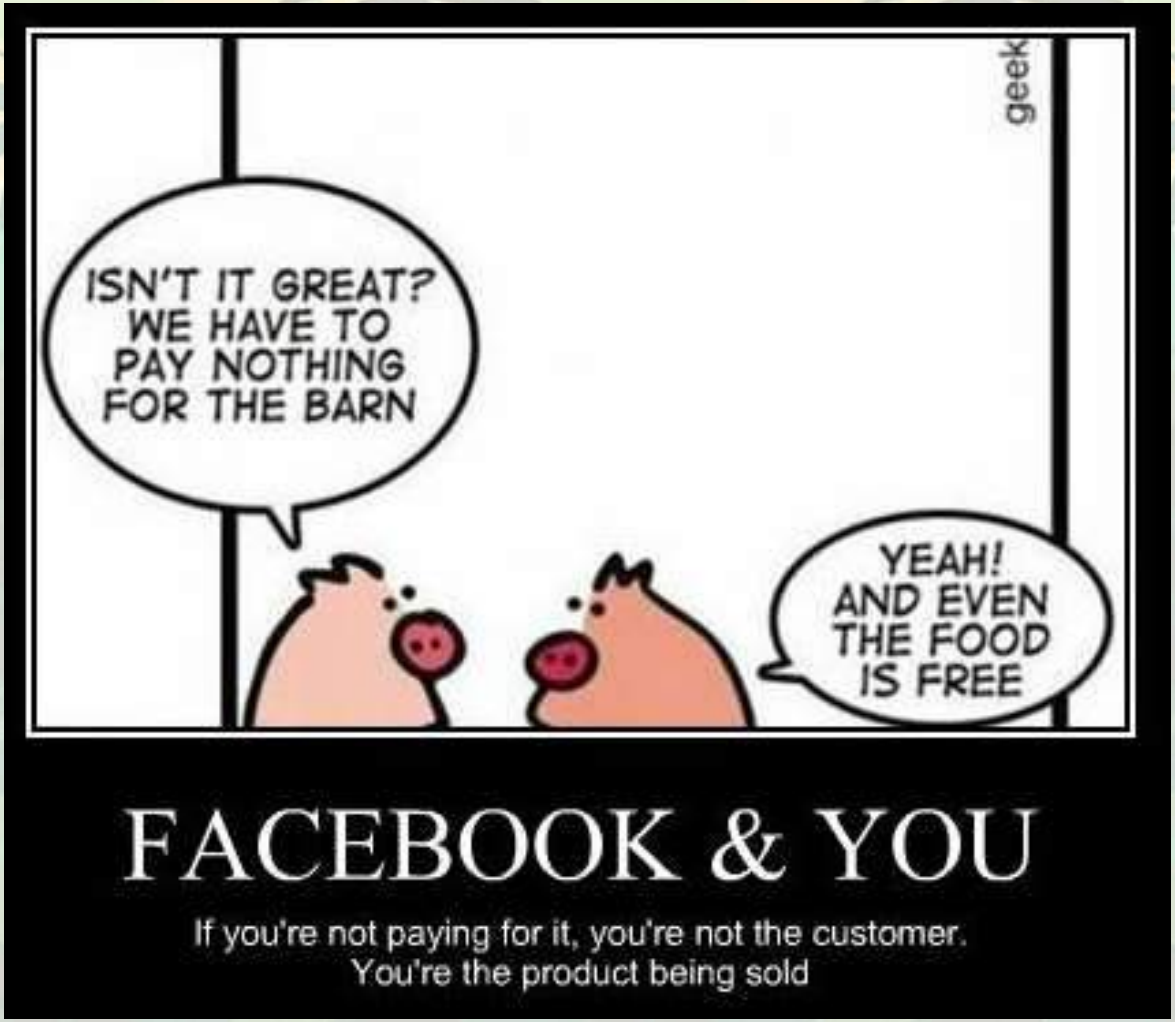
bruce.abernethy@protonmail.com




```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP.js v2.3.8
Comment: http://openpgpjs.org

xsBNBFkQ9dcBCADM9qNu8YgSZhvaw7q/h6L61DXS7l+rsFEazEMtD5P/NTVV
B/VKfnO3sXGhNs1hsGkpHtdTgfwhVkh9og5oDISlRupnH262rlP/3fqwQ9Zx
fDalY41IxBk2UgiL8+oDqY85YeJyGuCmLC+S/p/fBBKQn2qO1IL+NDg/C6kM
HrfZebIEwEy9NxCInfU5xshIftwnOzniyzYa1XMcri1A++LQm6pY9pq433fb
gvEtvcLNAAQyusutXFHNECwVn++jcntrY/G8/3OkrcDPwMumxCZRUwfXGrNm
anxF+VTGvCPpuHMoqgZMtJ+BSSEPCTY2wcemF5gYTUcDL4DfvenKn5Q5ABEB
AAHNP2JydWNlLmFiZXJuZXRoeUBwcm90b25tYWlsLmNvbSA8YnJ1Y2UuYWJl
cm5ldGh5QHByb3Rvbm1haWwuY29tPsLAdQQQAQgAKQUCWRD12AYLCQcIAwIJ
EH4Y4k7JFhhhBBUICgIDFgIBAhkBAhsDAh4BAABb6wf/Y6APqSlGPBHGvV6X
PPpyZLVOgVa6gQexLz/5pcRlaWHA4tb/bIzyWSh27Xq6KQkKEAi99uXEoDiw
fQbF2+gw0LDhUoOXV1Qh5ZVmuKrQt2G8gPlqqTk2M0NRjFemGtQt+/Gr5yCa
Tay/94jhyHaciCcJs4HHLT4yK90/xJZBfnUIkFxNegRGA0ZCe+gg7zQRXDcA
kBaKtUwk7aBiN4AHd2NlGt86k/HG/Aug98IZaA6ISm/SfiSEaJLp2jOb+FHs
z8PxjvzfveSZKKROamRxm9Vpspv66xkCdZKhrhG/P8cBsWL9S5tSddcZwh4V
lKzSvQ5cgbwj40EpuG3aM1siI87ATQRZEPXXAQgA0SKe1zscea92E3Bzfpmo
omcgDCsySpxdIwYHszXbi/OP76/fWxg4OVVq4vhBthfeUJjUQzcq/dUba6bc
oOiYPAJMttQlAbS3nPWJc43KFtuIlQPkk5z6BgMu3kSRXSAK1qJFimvro1ns
1/dZenq1nofmLsCLDPm6Y3VepZks6oTsbdgXbAoBo3D2v7Je76u+xlUc2ax0
g2VQo8oHXYvcw7e3BysrkyD4RkTYBw4m0YvqBSMSblRrXxnuTxyHOrQGPvSQ
1CfaRI4NuMd0AtKvJ9hIhNn+DxcswWkk/T+1yB3C+/ZEsHhVgGWTJOXnCfM8
R00OEbVJr3LmfI6g4MRHRwARAQABwsBfBBgBCAATBQJZEPXYCRB+GOJOyRYY
YQIbDAAAHs0H/1m3zx8W9KvXXz0Ue6Nbo59CP922EqEHhB7tIgikjQS3khko
OQcgtNnhXr2LhZvKVxJC202sLB268znWqgXLinzPUq7euqA2PiG9K9/e38Fv
euxcGoDPb7do0CQFOIbowMF7yBho2BYYHtA9pgi9bPjII1zs6XARIVRhIWRs
c3BsXFYfpk8yvo2ulX18iP5Yh1NV+p8quuZhrt6QCo1Qfpcam5kq4iQAiyBu
LALkalbBho6Ruk82SSXQO1Ks6zU95ZsAZT0xcUhKsCxMKIpx4fkblrH+l49c
x04fomhZg3vqiUVhxVDQGN9oJzUtOtmPtjLZ9jFAiyErBt8jvbfEsrg=

=9XpN

-----END PGP PUBLIC KEY BLOCK-----
```

"FREE" SERVICES

- There is no such thing as a free lunch.
- You are "paying" with your privacy, and security.



OTHER FUN THINGS … IF I TALK TOO FAST

- YubiKey
- BashBunny